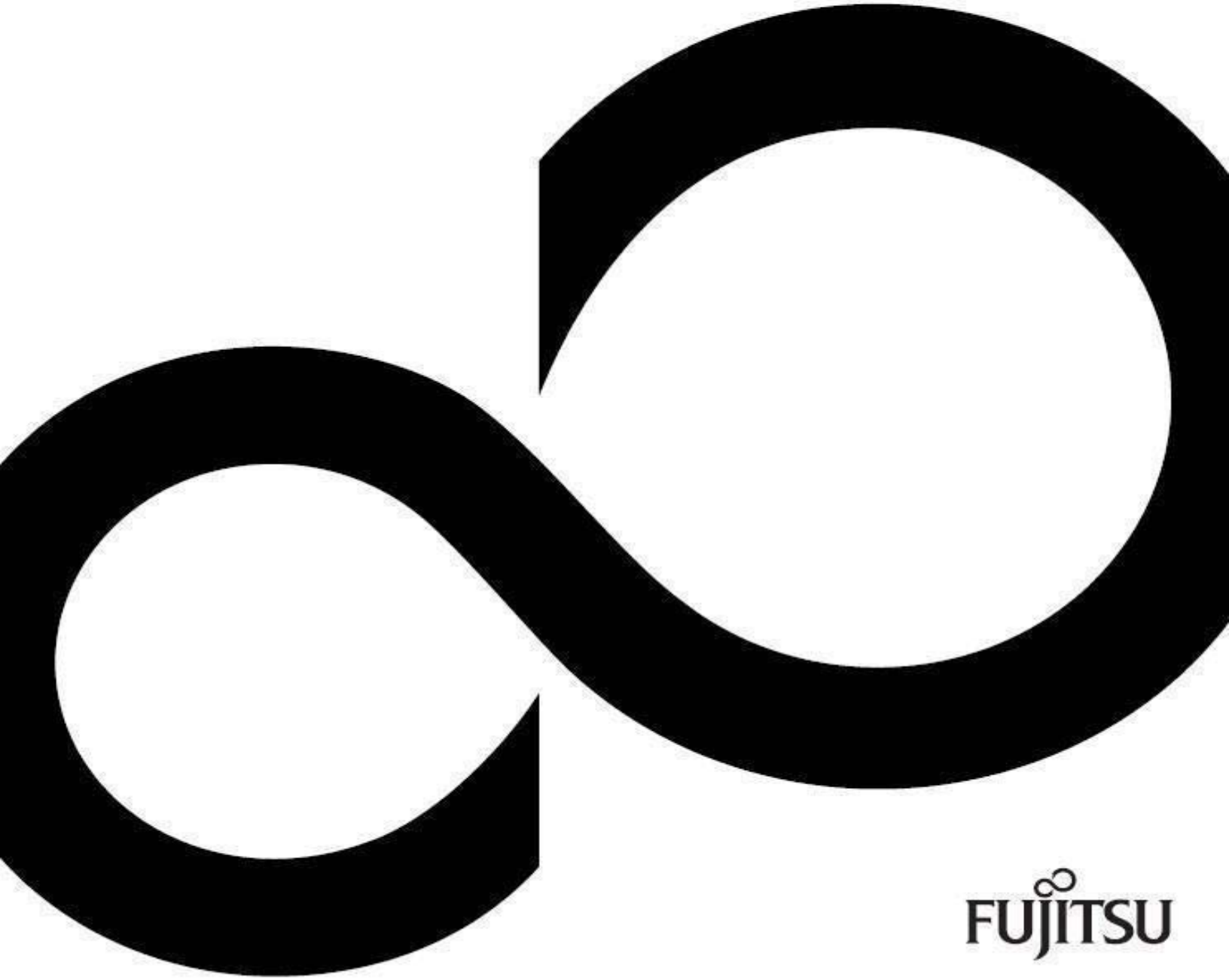
DeskView Version 10



FUJITSU

Notice

Fujitsu Technology Solutions DeskView 10.80

Copyright © 2006-2011 Fujitsu Technology Solutions and its third party licensors. All rights reserved.

Document Date: July 8, 2011

The content of this documentation is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Fujitsu Technology Solutions or Symantec. Fujitsu Technology Solutions or Symantec Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in this documentation.

DeskView is a trademark of Fujitsu Technology Solutions.

CELSIUS, FUTRO and SCENIC are registered trademarks of Fujitsu Technology Solutions.

ESPRIMO is a trademark of Fujitsu Technology Solutions.

ServerView® and PRIMERGY® are trademarks of Fujitsu Technology Solutions.

Altiris™, and the Altiris logo are trademarks of Symantec Corporation in the United States and other countries.

Microsoft, Windows, and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the United States and/or other countries.

All other brand names are trademarks or registered trademarks of their respective companies.

All other trademarks referenced are trademarks or registered trademarks of their respective owners, whose protected rights are acknowledged.

All rights, including rights of translation, reproduction by printing, copying or similar methods, in part or in whole, are reserved.

Offenders will be liable for damages.

All rights, including rights created by patent grant or registration of a utility model or design, are reserved.

Contents

Chapter 1: Introducing DeskView 6
About DeskView 6
What's new in DeskView 6
Products installed with DeskView 7
How DeskView works 7
What you can do with DeskView 7
Where to get more information 8

Chapter 2: Installing DeskView 10
System requirements 10
About DeskView requirements 10
About client computer requirements 10
Installing the DeskView product 11
Uninstalling DeskView 11
Uninstalling the DeskView agents from client computers 11
Uninstalling DeskView from the Notification Server computer 11

Chapter 3: Getting started with DeskView 12
About the Symantec Management Console 12
About the DeskView "Home" 12

Chapter 4: Preparing target systems from Fujitsu Technology Solutions for systems management 13
Preparing target systems for management 13
Discovering computers 14
Installing the Symantec Management Agent 14
Configuring the Symantec Management Agent settings for evaluation use 15
Installing DeskView agents 15
About upgrading existing DeskView Client 6.x software 16
Installing the DeskView Agent 16
Installing the Altiris Power Scheme Agent 17
Viewing DeskView agents installation reports 17

Chapter 5: Configuring DeskView 18
Importing a new Client Pack file 18
Configuring the Inventory Cache purging 18

Chapter 6: Using DeskView 19
About running tasks and policies 19
Viewing tasks and policies 19
Using DeskView Client Tools 20
Archiving and updating BIOS and BIOS settings 20
Using DeskView BIOS Management to harmonize BIOS settings in your environment 21
Configuring BIOS settings and enabling/disabling interfaces 22
Booting a computer from the network 24
Managing the power state of the client computer 25
Turning off client computers at a specific time 26
Updating drivers on the client systems 27

Changing power scheme settings . . . 27
Disabling mass storage devices . . . 28
Managing serial numbers . . . 29
Running DeskView Client Tools using a command line . . . 31
Using DeskView Alarm Management . . . 32
Configuring the Notification Server computer . . . 33
Selecting notifications . . . 33
Forwarding notifications by email . . . 34
Enabling DeskView notifications . . . 34
Configuring the notification settings . . . 34
Viewing DeskView notifications . . . 35
Viewing the system data of a DeskView managed system . . . 35
Accessing the Resource Manager . . . 37
Viewing DeskView inventory . . . 37
Viewing DeskView events . . . 37
Viewing DeskView System Data . . . 38

Chapter 7: Further help topics . . . 39
DeskView BIOS Management tool . . . 39
Archive BIOS task . . . 39
Update BIOS task . . . 41
Update BIOS settings task . . . 42
Initialize with Default values . . . 43
Update BIOS boot order . . . 43
Update BIOS supervisor password . . . 43
Update BIOS user password options (*) . . . 44
Update HardDisk password options (*) . . . 44
Update HDD password on boot options . . . 45
Update Password on boot options . . . 45
Update Trusted Platform Module (TPM) state (*) . . . 46
Update Trusted Platform Module hardware (*) . . . 46
Update 0-Watt PC options . . . 46
Update processor microcodes task . . . 47
DeskView Energy Management tool: Change Power State task . . . 48
DeskView Energy Management tool: Change power scheme settings task . . . 50
DeskView Driver Management tool: Update drivers task . . . 50
DeskView Security tool: Configure Mass Storage Access task . . . 51
DeskView Alarm Management . . . 52
DeskView Enable/Disable Notifications policy . . . 52
DeskView Configure Data Disk free space policy . . . 52
DeskView Configure System disk free space policy . . . 53
DeskView Configure Lease expiration policy . . . 53
Configure General Notification Email Forwarding page . . . 53
Configure General Notification Selection page . . . 54
DeskView Serial Numbers tool . . . 56
Apply imported serial numbers task . . . 56
Assign single serial number task . . . 56
Generate serial number task . . . 56
Manage serial numbers page . . . 57
DeskView System Data page . . . 58
DeskView Notifications page . . . 59
Cleanup Inventory Cache task . . . 60

Appendix A: Glossary 61

Index. 64

Chapter 1
Introducing DeskView

This chapter includes the following topics:

- *About DeskView*
- *What's new in DeskView*
- *Products installed with DeskView*
- *How DeskView works*
- *What you can do with DeskView*
- *Where to get more information*

About DeskView

DeskView is a client management software developed by Fujitsu Technology Solutions. Optimized for Fujitsu hardware, it helps to minimize the total cost of ownership of managing your client hardware infrastructure. Based on industry standards, DeskView manages STYLISTIC tablet PCs, ESPRIMO Mobile and LIFEBOOK Professional Notebooks, FUTRO Thin Clients, SCENIC and ESPRIMO Professional PCs, CELSIUS Workstations, and PRIMERGY servers. DeskView makes use of the features that are offered by the system for inventory management, system health monitoring, remote BIOS configuration and updates, and more. DeskView lets you manage your client infrastructure completely from your desk.

DeskView is comprised of the following components, which are installed as separate solutions. You can install and use only the selected solutions or all of them, depending on the needs specific for your organization.

Component	Description
DeskView for Business Clients	DeskView for Business Clients supports Fujitsu Technology Solutions systems running Microsoft Windows XP Professional and Windows 7. In addition to comprehensive hardware and software inventory, DeskView for Business Clients provides access to an extensive number of DeskView Client Tools.

What's new in DeskView

The following new features are introduced in the 10.80 release of DeskView:

- Support for the Symantec Management Platform 7.1 (64-bit Operating System)
- BIOS Management Features under one node
- One BIOS Settings Page for all available settings
- DeskView Diagnostics feature has been removed
- Single client Rollout without individual Discovery Agent

Products installed with DeskView

The Altiris management products that are installed and used with DeskView are shown in the following table:

Product	Description
Symantec Management Platform	The base management platform.
Altiris™ Real-Time Console Infrastructure	Provides out-of-band management tasks for computers with Intel AMT.
Altiris™ Power Scheme Task	This add-on lets you configure the client computer's power-saving options remotely.
Altiris™ Event Console	This add-on lets you collect SNMP and solution specific alerts to quickly respond to problems using automated actions.
Altiris™ Network Discovery	This add-on lets you discover devices in your network.
Altiris™ Pluggable Protocol Architecture	This add-on lets you communicate with and manage network devices suing different protocols required for your envionment.

How DeskView works

DeskView is a software that runs under the Symantec Management Platform software. DeskView lets you discover supported systems that are manufactured by Fujitsu Technology Solutions and install the DeskView Agent on these computers. The DeskView Agent communicates with the Symantec Management Platform and lets you perform management tasks from the Symantec Management Console.

What you can do with DeskView

With DeskView you can collect inventory data about client computers and view this inventory in the Symantec Management Console. DeskView lets you configure and update BIOS, run computer diagnostics, update drivers, and configure security settings remotely from the Symantec Management Console.

You can run these tasks on a collection of computers, immediately, or at a later time, also you can connect to a specific system from Fujitsu Technology Solutions directly, view live inventory data, and run management tasks in real time from the Symantec Management Console.

Where to get more information

Use the following documentation resources to learn and use this product.

Document	Description	Location
Release Notes	Information about new features and important issues. This information is available as an article in the Altiris Knowledge Base.	http://www.symantec.com/business/support/index?page=home You can search for the product name.
User's Guide	Information about how to use this product, including detailed technical information and instructions for performing common tasks. This information is available in PDF format.	• The Documentation Library, which is available in the Symantec Management Console on the Help menu. • The Product Support page, which is available at the following URL: http://www.symantec.com/business/support/all_products.jsp When you open your product's support page, look for the Documentation link on the right side of the page.
Help	Information about how to use this product, including detailed technical information and instructions for performing common tasks. Help is available at the solution level and at the suite level. This information is available in HTML help format.	The Documentation Library, which is available in the Symantec Management Console on the Help menu.
DeskView Client 6 User Manual	Information about the DeskView Client Tools command-line parameters and output codes. This information is available in PDF format.	• The Documentation Library, which is available in the Symantec Management Console on the Help menu. • The Fujitsu Technology Solutions Web site: http://ts.fujitsu.com/solutions/it_infrastructure_solutions/manageability/deskview_downloads.html

In addition to the product documentation, you can use the following resources to learn about Altiris products.

Resource	Description	Location
Altiris Knowledgebase	Articles, incidents, and issues about Altiris products.	http://www.symantec.com/business/support/index?page=home
Altiris Juice	An online magazine that contains best practices, tips, tricks, and articles for users of Altiris products.	http://www.altiris.com/juice/
Online Forums	Forums for users of Altiris products.	http://forums.altiris.com/

Chapter 2
Installing DeskView

This chapter includes the following topics:

- *System requirements*
- *Installing the DeskView product*
- *Uninstalling DeskView*

System requirements

DeskView has the following system requirements:

- DeskView installation requirements
  See About DeskView requirements on page 10.
- DeskView Agent installation requirements
  See About client computer requirements on page 10.

About DeskView requirements

DeskView requires the following:

- Symantec Management Platform 7.1

For more information on Symantec Management Platform prerequisites and installation instructions, see the *Symantec Management Platform Help*.

See Where to get more information on page 8.

About client computer requirements

The DeskView Agent can only be installed and run on the following systems from Fujitsu Technology Solutions:

- Tablet PCs
- Notebooks
- Professional PCs
- Workstations

The DeskView Agent supports Windows XP Professional and Windows 7 operating systems.

For a list of supported systems please see also our Manageability & Security Feature Finder at

http://www.ts.fujitsu.com/solutions/it_infrastructure_solutions/manageability/featurefinder.html.

Installing the DeskView product

Use Symantec Installation Manager to install DeskView.

For more information on installing products, see the *Symantec Management Platform Installation Guide*.

Uninstalling DeskView

To uninstall DeskView, perform the following steps:

Step	Action	Description
Step 1	Uninstall the DeskView agents from client computers.	This step is required if you do not want to reinstall DeskView later. See Uninstalling the DeskView agents from client computers on page 11.
Step 2	Uninstall DeskView from the Notification Server computer.	This step removes the product from the Notification Server computer. See Uninstalling DeskView from the Notification Server computer on page 11.

Uninstalling the DeskView agents from client computers

Agent uninstall policies let you remove the DeskView agents from supported client computers. Remove the agents if you do not want to reinstall DeskView later.

The agent's uninstall process can take some time to start, depending on the intervals that are set between updates of the Symantec Management Agent.

See Configuring the Symantec Management Agent settings for evaluation use on page 15.

We recommend that you do not uninstall the DeskView software from Notification Server until the agent uninstall tasks have run on all client computers. When DeskView is uninstalled, there is no automated way to uninstall the agents.

To uninstall the DeskView Agent

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Agents and Plug-ins > DeskView Agent - Uninstall**.
3. Turn on the policy (To turn on the policy, at the upper right of the page, click the colored circle, and then click **On**).
4. Click **Save changes**.

Uninstalling DeskView from the Notification Server computer

Use Symantec Installation Manager to uninstall DeskView.

For more information on uninstalling products, see the *Symantec Management Platform Installation Guide*.

Chapter 3
Getting started with DeskView

This chapter includes the following topics:

- *About the Symantec Management Console*
- *About the DeskView "Home"*

About the Symantec Management Console

You perform all DeskView configuration and administration tasks in the Symantec Management Console.

The Symantec Management Console is the Web-browser-based administration console for working with Notification Server and Symantec solutions, including DeskView. The console lets you perform tasks, schedule events, run reports, perform configuration, configure security, and more. You can run the console from the Notification Server computer (locally) or from a remote computer with a network connection to the Notification Server computer. This means you can perform administration tasks from wherever you are.

The console lets you set security specific to each console user. You specify which areas of the console a user has access to and the rights a user has to perform specific actions. For example, one user can run reports while another user can only view the reports that have already been run.

For more information on the console, see the Symantec Management Platform documentation, which can be accessed through the console's Help menu.

You can start the console remotely by typing the following URL into Internet Explorer's address bar: `http://<Notification_Server_name>/altiris/console`

About the DeskView "Home"

DeskView provides a home page that introduces you to DeskView components and provides links to common tasks.

To open the DeskView home page, in the Symantec Management Console, on the Home menu, click **DeskView**.

Chapter 4
Preparing target systems from Fujitsu Technology Solutions for systems management

This chapter includes the following topics:

- *Preparing target systems for management*
- *Discovering computers*
- *Installing the Symantec Management Agent*
- *Configuring the Symantec Management Agent settings for evaluation use*
- *Installing DeskView agents*
- Viewing DeskView agents installation reports

Preparing target systems for management

The following is the recommended way of preparing target computers for management:

Step	Action	Description
Step 1	Discover manageable computers in your environment.	Discovery lets you find computers on which you can install the Symantec Management Agent. See Discovering computers on page 14.
Step 2	Install the Symantec Management Agent to the client computers.	The Symantec Management Agent lets Notification Server get information from and interact with the client computers. See Installing the Symantec Management Agent on page 14.
Step 3	(Optional) Configure the Symantec Management Agent settings for evaluation use.	For easier configuration and evaluation of DeskView, you can make the Symantec Management Agent to request configuration from Notification Server more frequently. See Configuring the Symantec Management Agent settings for evaluation use on page 15.
Step 4	Install DeskView agents.	Install the DeskView management software to supported systems from Fujitsu Technology Solutions in your environment. See Installing DeskView agents on page 15.

Discovering computers

Discovery lets you find the hostnames of the computers where you can install the Symantec Management Agent. You can discover computers on the network using a domain or a workgroup search.

For more information on resource discovery, see the *Symantec Management Platform Help*.

See Preparing target systems for management on page 13.

To discover computers

1. In the Symantec Management Console, on the Actions menu, click **Discover > Import Domain Membership/WINS**.
2. In the Add Domain box, type the domain name, and then click the **Add** symbol.
3. Check **Domain Membership** and click **Discover Now**.
4. As the discovery process finishes, click **View discovery reports**.
5. Open a report to view the list of discovered computers.
   For example, right-click the **Discovered Computers** report, and then click **Open**.

Installing the Symantec Management Agent

The Symantec Management Agent is a program that you install on the computers you want to manage, allowing the Symantec Management Platform and solutions to get information from and interact with your computers. The agent enables computers to receive configuration information from and send data to Notification Server and helps download packages as well as tasks and jobs. The agent lets you change settings on the managed computer and install and manage various solution-specific plug-ins.

You must install the Symantec Management Agent on the computers you want to manage with DeskView.

For more information on the Symantec Management Agent, see the *Symantec Management Platform Help*.

See Preparing target systems for management on page 13.

To install the Symantec Management Agent

1. In the Symantec Management Console, on the Actions menu, click **Agents/Plug-ins > Push Symantec Management Agent**.
2. On the Symantec Management Agent Installation page, install the Symantec Management Agent to computers in your environment.
   For more information on how to install the Symantec Management Agent, see the *Symantec Management Platform Help* (Press **F1** or click **Help > Context** in the Symantec Management Console).

Configuring the Symantec Management Agent settings for evaluation use

(Optional)

By default, the Symantec Management Agent requests new configuration from Notification Server once per hour. This means that it can take up to one hour for a rollout policy (for example, the DeskView Discovery Agent - Install policy) to reach the target computer.

If you are evaluating this solution in a lab environment, you can change the configuration request interval to speed up the evaluation process.

The next time the Symantec Management Agent downloads configuration information, these settings will take effect. If you were using the default agent configuration values before the change, updates can take up to one hour before these changes are effective.

See Preparing target systems for management on page 13.

To configure the Symantec Management Agent for evaluation use

1. In the Symantec Management Console, on the Settings menu, click **Agents/Plug-ins > Targeted Agent Settings**.
2. In the left pane, under Policy Name, click the policy that applies to the computers that you want to configure.
   For example, click **All Desktop computers (excluding 'Site servers')**.
3. On the General tab, in the Download new configuration every box, change the value to 5 minutes.
   This forces the agent to check more frequently for changes so you can see the results of the changes that you make more quickly.
4. In the Upload basic inventory every box, change the value to 15 minutes.
   This forces inventory data to be sent more frequently.
5. Click **Save changes**.

Installing DeskView agents

DeskView agents let the DeskView solution gather different type of information from and interact with the client systems.

See Preparing target systems for management on page 13.

Install the agents that are shown in the following table:

Agent	Description
DeskView Agent	This agent installs DeskView Client software on the client systems and is required for the DeskView solution to communicate with the client systems from Fujitsu Technology Solutions. See Installing the DeskView Agent on page 16. Also see About upgrading existing DeskView Client 6.x software on page 16.
Altiris Power Scheme Agent	This is an optional agent. Install this agent if you want to configure power scheme settings on the client systems. See Installing the Altiris Power Scheme Agent on page 17.

About upgrading existing DeskView Client 6.x software

It is possible to deploy the latest DeskView Agent on a system where a DeskView Client version 6.x is already installed. When deploying the DeskView Agent with the rollout policy, the complete current DeskView Client 6.x version is automatically uninstalled and then, without a restart, the DeskView Client 6.x and the DeskView Agent are installed on the target computer.

However, the rollout policy cannot automatically uninstall DeskView Client 6.x if this software was manually installed outside of Notification Server. In this case, you must manually uninstall DeskView Client 6.*x* from the computers to which you want to roll out the DeskView Agent.

See Installing DeskView agents on page 15.

Installing the DeskView Agent

The DeskView Agent is a client software package that includes a DeskView Agent as well as the DeskView Client tools. You can deploy this package remotely on the manageable systems from Fujitsu Technology Solutions using the DeskView Agent - Install policy.

Before you install the DeskView Agent, you must discover systems from Fujitsu Technology Solutions.

See Installing DeskView agents on page 15.

To install the DeskView Agent

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Agents and Plug-ins > DeskView Agent - Install**.
3. If you want to reinstall the existing DeskView client components, check **Force existing components reinstallation**.
   This is useful when you want to repair the DeskView components that are already installed on the client system.

4. Sometimes a restart is required to complete the installation or upgrade of the DeskView Agent. If you want to restart the target system after running the task, under Power Management, check **Restart the computer after task**.
5. If you want, under **Applied To**, edit the targets to which the policy is applied.
6. Turn on the policy.
   To turn on the policy, at the upper right of the page, click the colored circle, and then click **On**.
7. Click **Save changes**.

Installing the Altiris Power Scheme Agent

The Altiris Power Scheme Agent is an add-on to the Symantec Management Agent that lets you configure power scheme settings of the target computers.

See Installing DeskView agents on page 15.

To install the Altiris Power Scheme Agent

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Getting Started > DeskView for Business Clients Getting Started > 1. Getting Started > Step 4. Install Power Scheme Agent**.
3. Turn on the policy.
   To turn on the policy, at the upper right of the page, click the colored circle, and then click **On**.
4. Click **Save changes**.

Viewing DeskView agents installation reports

DeskView includes reports that provide information about the status of the DeskView agents on your client computer. These reports provide installation and execution status of the agents as well as the agents version information.

See Preparing target systems for management on page 13.

To view the DeskView agents installation status reports

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Reports > Business Clients > Installation**.
3. Click a report.
   For example, click the **Installation Status DeskView Agents** report.

Chapter 5
Configuring DeskView

This chapter includes the following topics:

- *Importing a new Client Pack file*
- *Configuring the Inventory Cache purging*

Importing a new Client Pack file

DeskView provides you with the ability to import multiple DeskView client pack files in order to roll them out to the computers in your environment.

To import the a new Client Pack File

1. If available, you can download the a new Client Pack File to a temporary location on your computer.
2. In the Symantec Management Console, on the Home menu, click **DeskView**.
3. In the left pane, click **Configuration > Import Client Pack File**.
4. In the right pane, type the path to the file that you downloaded, or click **Browse** to browse for the file.
5. Click **Import**.

Configuring the Inventory Cache purging

DeskView uses an inventory cache folder (by default, C:\Program Files\DeskView\InventoryCache) to store inventory information events that are received from managed systems before the events get processed by DeskView. After DeskView processes the inventory from a managed system, the corresponding event file is deleted. However, if DeskView cannot process inventory events, the events can be accumulated infinitely. To prevent an out-of-space situation on the disk, the Cleanup Inventory Cache task monitors the size of the inventory cache folder and maintains its size according to parameters that you specify.

By default, the task is configured to run daily. When the conditions you specified are met, the cached data is purged.

To configure the Inventory Cache purging

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Configuration > Cleanup Inventory Cache task**.
3. In the right pane, configure the settings.
   For help, in the Symantec Management Console, press **F1** or click **Help > Context**.

Chapter 6
Using DeskView

This chapter includes the following topics:

- *About running tasks and policies*
- *Using DeskView Client Tools*
- *Running DeskView Client Tools using a command line*
- *Using DeskView Alarm Management*
- *Viewing the system data of a DeskView managed system*

About running tasks and policies

You can run DeskView tools using tasks or task-based policies.

If you want a tool to run immediately or on a specific schedule, use tasks to run the tool.

However, the peculiarity of the task is the following: If a client computer happens to be offline or turned off at the time the task is scheduled to run, the task will fail to run on that computer.

If you want to make sure that, sooner or later, all computers run the tool, use task-based policies. When task-based policies are turned on, they are active at all times. When a computer that is turned off comes back online, it receives and executes the policy.

See Viewing tasks and policies on page 19.

Viewing tasks and policies

You can run DeskView tools using tasks or task-based policies.

See About running tasks and policies on page 19.

To view tasks

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Tasks**.

To view task-based policies

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Policies**.

Using DeskView Client Tools

When you install the DeskView Agent on client computers, the DeskView BIOS Management, DeskView Driver Management, DeskView Energy Management, DeskView Security, and DeskView Inventory Management client tools are installed as part of that installation.

DeskView solution includes the following tools:

DeskView Tool	Description
DeskView BIOS Management	Lets you archive and update the BIOS of the target system and change BIOS settings on the target system. See Archiving and updating BIOS and BIOS settings on page 20.
DeskView Driver Management	Lets you update the drivers on the target system. See Updating drivers on the client systems on page 27.
DeskView Energy Management	Lets you manage power-saving schemes on the target systems. See Changing power scheme settings on page 27.
DeskView Security	Lets you disallow connecting mass storage devices to the target systems. See Disabling mass storage devices on page 28.
DeskView Inventory Management	Lets you manage serial numbers of the target systems. See Managing serial numbers on page 29.

Archiving and updating BIOS and BIOS settings

The DeskView BIOS Management tool lets you perform the following tasks remotely on client computers:

- Archive the BIOS
- Update the BIOS
- Update the BIOS settings
- Update processor microcodes

DeskView BIOS Management supports the .omf, .ocf, and .bup file formats for BIOS files.

The DeskView BIOS Management tool lets you make BIOS settings the same on all computers in your environment.

See Using DeskView BIOS Management to harmonize BIOS settings in your environment on page 21.

Note
You must run DeskView BIOS Management tools under an administrative user account.

Warning
When a DeskView BIOS Management tool runs on a mobile system, the tool checks if the system is plugged into the power source and if the system's battery charge level is more than 33%. If these conditions are not met, DeskView BIOS Management aborts the action and reports an error.

To run a DeskView BIOS Management task

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Tasks > DeskView BIOS Management**.
3. Click the task you want to run.
4. In the right pane, configure the task.
   For help, in the Symantec Management Console, press **F1** or click **Help > Context**.
5. Run the task one time or on a schedule.
   For information on running tasks, see the *Symantec Management Platform Help.*

To run a DeskView BIOS Management task-based policy

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Policies > DeskView BIOS Management**.
3. Select the policy you want to run.
4. In the right pane, configure the settings.
   For help, in the Symantec Management Console, press **F1** or click **Help > Context**
5. Configure the scheduling options.
6. Turn on the policy.
   To turn on the policy, at the upper right of the page, click the colored circle, and then click **On**.
7. Click **Save changes**.

Using DeskView BIOS Management to harmonize BIOS settings in your environment

You can use the DeskView BIOS Management tools to harmonize BIOS settings in your environment by creating a reference BIOS and distributing it throughout your systems.

To harmonize BIOS settings

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. Do one of the following:
   - If you want to use a task, in the left pane, click **Tasks > DeskView BIOS Management > Archive BIOS**.
   - If you want to use a task-based policy, in the left pane, click **Policies > DeskView BIOS Management > DeskView Archive BIOS policy**.

   See About running tasks and policies on page 19.
3. Under BIOS Archive File, choose a path where you want to save the BIOS archive file.
   If you choose to save the archive file to a custom directory, we recommend that you

use a network share that client computers can access.
Example: `\\server\share`

4. Click **Specify name or pattern** and type a name for the BIOS archive file. Remember the name.
   For more information on the name formats, see Archive BIOS task on page 39.
5. Run the task or the policy on the computer that you want to use as a reference.
6. After the task or the policy has run, do one of the following:
   - If you want to use a task, in the left pane, click **Tasks > DeskView BIOS Management > Update BIOS**.
   - If you want to use a task-based policy, in the left pane, click **Policies > DeskView BIOS Management > DeskView Update BIOS policy**.
     See About running tasks and policies on page 19.
7. On the Update BIOS page:
   - Click **Get BIOS Update Files from** and type the network share where you saved the file in step 4.
     Example: `\\server\share`
     DeskView can detect BIOS archive files automatically; however, if you want, you can click **Specify filename** and type the BIOS archive file name manually.
8. (Optional) Configure other settings.
   See Update BIOS settings task on page 42.
9. Click **Save changes**.
10. Run the task or the policy on the computers with the same hardware as on the reference computer.

Configuring BIOS settings and enabling/disabling interfaces

The DeskView BIOS Settings tool lets you perform the following tasks remotely on client computers:

- Set BIOS settings to default values.
- Change boot order.
- Update the BIOS supervisor password.
- Update the BIOS user password. (*)
- Update the hard disk password. (*)
- Force the user to enter HDD Password on boot
- Force the User to enter Password on boot
- Enable/disable the bluetooth controller.
- Enable/disable the floppy disk controller.
- Allow/disallow flashing BIOS.
- Enable/disable the infrared controller.
- Allow/disallow network boot using BOOTP or PXE.
- Enable/disable the parallel port controller.
- Enable/disable the USB host controller.

- Allow/disallow starting the computer with Wake on LAN.
- Enable/disable the wireless interface.
- Enable (Green PC) or disable the 0-Watt PC option or set an interval for remote management.
- Activate or deactivate the Audio Controller.
- Enable or disable Hyper-Threading.
- Enable or disable the boot menu (F12).
- Show/hide BIOS boot process diagnostic display
- Configure USB 1.1 / 2.0 support.
- Enable or disable the USB ports on the front of the computer.
- Enable or disable the USB ports on the rear of the computer.
- Determine how the unused USB ports should be processed based on device categories.
- Configure USB Legacy support.
- Enable or disable core multiprocessor functionality.
- Enable or disable Enhanced Intel SpeedStep Technology.
- Enable or disable Enhanced Idle Power State (additional power settings).
- Enable or disable Turbo Boost Technology.
- Enable or disable internal camera.
- Enable or disable the BIOS information message that the F2 key can be used during boot-up to jump into BIOS.
- Enable or disable the ability to boot from removable media.
- Enable or disable the Low Power Soft Off support.
- Enable or disable DASH support.
- Enable or disable hardware virtualisation.
- Enable or disable Non-Execution memory protection.
- Configure the PS/2 mouse configuration options.
- Enabled or disable the keyboard check during Boot.
- Allow/Disallow TPM automated physical presence. (*)
- Enable/Disable TPM state. (*)
- Enable/Disable Trusted Platform Module hardware. (*)

(*) In order to be able to use these functions it is necessary to contact "Deskview.Consulting@ts.fujitsu.com"

For example, you can use the DeskView BIOS Settings tools to boot a computer from the network.

See Booting a computer from the network on page 24.

To run a DeskView BIOS Settings task

1. In the Symantec Management Console, on the Home menu, click **DeskView**.

2. In the left pane, click **Tasks > DeskView BIOS Management > Update BIOS Settings**.
3. Select the appropriate BIOS settings.
4. Run the task one time or on a schedule.
   For information on running tasks, see the *Symantec Management Platform Help.*

To run a DeskView BIOS Settings task-based policy

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Policies > DeskView BIOS Management > DeskView Update BIOS Settings policy**.
3. Select the appropriate BIOS settings.
4. Click the policy you want to run.
5. In the right pane, configure the settings.
   For help, in the Symantec Management Console, press **F1** or click **Help > Context**
6. Configure the scheduling options.
7. Turn on the policy.
   To turn on the policy, at the upper right of the page, click the colored circle.
8. Click **Save changes**.

Booting a computer from the network

You can use DeskView BIOS Settings tasks to boot computers from a PXE server. To do this, first you run the Update LAN remote boot task to enable PXE boot, then you run the Update BIOS boot order task to change the boot order, and then you restart the computer. You can run all these tasks remotely from the Symantec Management Console, without touching the client system.

To boot a computer from the network

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Tasks > DeskView BIOS Management > Update BIOS Settings**.
3. If required, type the BIOS password.
4. Click the checkbox next to the **LAN remote boot** option.
5. Change the drop down to select the **Enable** option.
6. Click **Save changes**.
7. Run the task.
   For information on running tasks, see the *Symantec Management Platform Help.*
8. After the task has run successfully, in the left pane, click **Tasks > DeskView Energy Management > Change Power State**.
9. Under DeskView Energy Management Command, click **Restart computer**.
10. If you want to close all open applications, losing all unsaved data, check **Terminate all applications currently running without query**.
11. Click **Save changes**.

12. Run the task on the same computer.
    For information on running tasks, see the *Symantec Management Platform Help.*
13. After the task has run successfully, in the left pane, click **Tasks > DeskView BIOS Management > Update BIOS Settings.**
14. If required, type the BIOS password.
15. Click the checkbox next to the **Bios Boot Order** option.
16. Under Boot sequence, in the Applied Devices box, click **Network (e.g. PXE/ BOOTP)**, and then click the **Move up** button until the selected device is at the top of the list.
17. Click **Save changes**.
18. Run the task on the same computer.
    For information on running tasks, see the *Symantec Management Platform Help.*
19. After the task has run successfully, in the left pane, click **Tasks > DeskView Energy Management > Change Power State**.
20. Under DeskView Energy Management Command, click **Restart computer**.
21. If you want to close all open applications, losing all unsaved data, check **Terminate all applications currently running without query**.
22. Click **Save changes**.

Run the task on the same computer.
For information on running tasks, see the *Symantec Management Platform Help.*

Managing the power state of the client computer

The DeskView Energy Management - Change Power State tool lets you perform the following tasks remotely on client computers:

- Restart the computer
- Turn off the computer
- Switch the computer into hibernate mode (works only if the hibernate mode is enabled)
- Switch the computer into standby mode

For example, you can use DeskView Energy Management to reduce energy usage in your enterprise by turning off the computers at a specific time.

See Turning off client computers at a specific time on page 26.

If you turn off or restart a client computer that has an application open, the user will be notified about the shutdown and prompted to save his work. You also have an option to force closing all applications without saving.

To run a DeskView Energy Management - Change Power State task

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Tasks > DeskView Energy Management > Change Power State**.
3. In the right pane, configure the task.
   For help, in the Symantec Management Console, press **F1** or click **Help > Context**

4. Run the task one time or on a schedule.
   For information on running tasks, see the *Symantec Management Platform Help.*

To run a DeskView Energy Management - Change Power State task-based policy

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Policies > DeskView Energy Management > DeskView Change Power State policy**.
3. In the right pane, configure the settings.
   For help, in the Symantec Management Console, press **F1** or click **Help > Context**
4. Configure the scheduling options.
5. Turn on the policy.
   To turn on the policy, at the upper right of the page, click the colored circle, and then click **On**.
6. Click **Save changes**.

Turning off client computers at a specific time

You can use DeskView Energy Management to reduce energy usage in your enterprise by turning off the computers at a specific time.

To turn off client computers at a specific time

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Tasks > DeskView Energy Management > Change Power State**.
3. On the Change power state page, under DeskView Energy Management Command, click **Shutdown computer**.
4. If you want to close all open applications, losing all unsaved data, check **Terminate all applications currently running without query**.
5. By default, the tool will run under the Symantec Management Agent credentials. If you want to run the tool under a different user, click **Advanced** and configure a different user.
6. Under Task Status, on the toolbar, click **New Schedule**.
7. On the New Schedule page, under Schedule, click **Schedule**.
8. Click **At date/time**.
9. (Optional) Modify the date.
10. Specify the time when you want to turn off the computers, for example, 21:00.
11. If you want to repeat this task every day, check **Repeat every** and then select **1** and select **Days**.
12. Under Input, on the toolbar, on the Add menu, click **Target**.
13. Under Filtering rules, click **Add rule**, click **exclude computers not in**, click **Filter**, and select the computer filter you want the task to run on.
    To search for a filter, start typing the first characters of the filter's name. For example, to search for the Professional PCs filter in the list, type `prof` and then select Professional PCs from the drop-down list.

Computers currently matching the filtering rules you created appear in the list. The task will run on these computers.

14. Click **OK**.
15. Click **Schedule**.
16. Under Task Status, monitor the task's execution.
    For information on running tasks, see the *Symantec Management Platform Help.*

Updating drivers on the client systems

For a stable network, it is indispensable that the system drivers of the client computers are always kept up to date.

With DeskView you can easily update the drivers in two ways:

- Using the Fujitsu Technology Solutions Web site where the drivers are always kept actual
- Using the Fujitsu Technology Solutions Driver and Utility DVD or CD, which contain the driver versions you need for your clients

The DeskView Driver Management tool lets you update system drivers on client computers remotely from the Symantec Management Console.

To run a DeskView Driver Management task

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Tasks > DeskView Driver Management > Update drivers**.
3. In the right pane, configure the task.
   For help, in the Symantec Management Console, press **F1** or click **Help > Context**
4. Run the task one time or on a schedule.
   For information on running tasks, see the *Symantec Management Platform Help.*

To run a DeskView Driver Management task-based policy

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Policies > DeskView Driver Management > DeskView Update drivers policy**.
3. In the right pane, configure the settings.
   For help, in the Symantec Management Console, press **F1** or click **Help > Context**
4. Configure the scheduling options.
5. Turn on the policy.
   To turn on the policy, at the upper right of the page, click the colored circle, and then click **On**.
6. Click **Save changes**.

Changing power scheme settings

The DeskView Energy Management tool lets you activate the custom power scheme remotely on client computers. You can also run the task on schedule (for example, at

system startup) to ensure the power options are always set according to your company's energy policy.

We recommend that you use the default power-saving settings provided by the DeskView Change power scheme settings task/policy for optimum power saving and performance.

Before you can use the DeskView Energy Management tool, you must install the Power Scheme Agent to client computers.

See Installing the Altiris Power Scheme Agent on page 17.

To run a DeskView Energy Management task

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Tasks > DeskView Energy Management**> **Change power scheme settings.**
3. In the right pane, configure the task.
   For help, in the Symantec Management Console, press **F1** or click **Help > Context**
4. Run the task one time or on a schedule.
   For information on running tasks, see the *Symantec Management Platform Help.*

To run a DeskView Energy Management task-based policy

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Policies > DeskView Energy Management**> **DeskView Change power scheme settings policy**.
3. In the right pane, configure the settings.
   For help, in the Symantec Management Console, press **F1** or click **Help > Context**
4. Configure the scheduling options.
5. Turn on the policy.
   To turn on the policy, at the upper right of the page, click the colored circle, and then click **On**.
6. Click **Save changes**.

Disabling mass storage devices

The DeskView Security tool lets you restrict usage of USB mass storage devices (Windows XP) and removable disks (Windows 7). You can use this task to prevent data larceny and unintentional bringing in of extraneous software, like viruses or games, from removable storage devices. You can lock the devices completely or set to read-only.

To run a DeskView Security task

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Tasks > DeskView Security**.
3. Click the task you want to run.
4. In the right pane, configure the task.
   For help, in the Symantec Management Console, press **F1** or click **Help > Context**

5. Run the task one time or on a schedule.
   For information on running tasks, see the *Symantec Management Platform Help.*

To run a DeskView Security task-based policy

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Policies > DeskView Security**.
3. Click the policy you want to run.
4. In the right pane, configure the settings.
   For help, in the Symantec Management Console, press **F1** or click **Help > Context**
5. Configure the scheduling options.
6. Turn on the policy.
   To turn on the policy, at the upper right of the page, click the colored circle, and then click **On**.
7. Click **Save changes**.

Managing serial numbers

The DeskView Serial Numbers tool lets you write your own serial numbers remotely into the BIOS of the client computers. You can let DeskView generate the serial numbers or you can import your own list of numbers.

With the DeskView Serial Numbers tool you can perform the following tasks:

- View serial numbers you assigned to systems.
- Assign a serial number to a single system.
- Assign serial numbers using a pattern to multiple systems.
- Import the list of serial numbers from a .csv file, and assign the numbers to multiple systems.

To view assigned serial numbers

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Configuration > Manage Serial Numbers**.
3. Click **View serial numbers**.
4. Click **Next**.

To assign a serial number to a single system

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. Do one of the following:
   - If you want to use a task, in the left pane, click **Tasks > DeskView Inventory Management > Assign single serial number**.
   - If you want to use a task-based policy, in the left pane, click **Policies > DeskView Inventory Management> DeskView Assign single serial number policy**.

   See About running tasks and policies on page 19.

3. In the right pane, configure the settings.
   For help, in the Symantec Management Console, press **F1** or click **Help > Context**
4. Do one of the following:
   - If you are using the task, run the task one time or on a schedule.
     For information on running tasks, see the *Symantec Management Platform Help.*
   - If you are using the task-based policy, configure the scheduling options, turn on the policy, and click **Save changes**.

To assign serial numbers using a pattern to multiple systems

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. Do one of the following:
   - If you want to use a task, in the left pane, click **Tasks > DeskView Inventory Management > Generate serial number**.
   - If you want to use a task-based policy, in the left pane, click **Policies > DeskView Inventory Management > DeskView Generate serial number policy**.

   See About running tasks and policies on page 19.
3. In the right pane, configure the settings.
   For help, in the Symantec Management Console, press **F1** or click **Help > Context**
4. Do one of the following:
   - If you are using the task, run the task one time or on a schedule.
     For information on running tasks, see the *Symantec Management Platform Help.*
   - If you are using the task-based policy, configure the scheduling options, turn on the policy, and click **Save changes**.

To import the list of serial numbers from a .csv file and assign the numbers to multiple systems

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Configuration > Manage Serial Numbers**.
3. On the Manage Serial Numbers page, click **Export serial numbers**.
4. Click **Next**.
5. Select a filter that contains the computers you want to export.
   For example, select the "All DeskView managed systems" filter.
6. Click **Next**.
7. Click the **here** link to download the list of computers.
8. Click **Finish**.
9. Open the .csv file you downloaded in a text editor and populate the file with serial numbers.
   Serial numbers are located in the second column of the .csv file. The serial numbers must contain only alphanumeric characters.
10. On the Manage Serial Numbers page, click **Import serial numbers**.

11. Click **Next**.
12. Browse to the .csv file you edited in step 9.
13. Click **Next**.
14. Do one of the following:
    - If you want to use a task, in the left pane, click **Tasks > DeskView Inventory Management > Apply imported serial numbers**.
    - If you want to use a task-based policy, in the left pane, click **Policies > DeskView Inventory Management > DeskView Apply imported serial numbers policy**.

    See About running tasks and policies on page 19.
15. Do one of the following:
    - If you are using the task, run the task one time or on a schedule.
      For information on running tasks, see the *Symantec Management Platform Help.*
    - If you are using the task-based policy, configure the scheduling options, turn on the policy, and click **Save changes**.

Running DeskView Client Tools using a command line

The DeskView software contains a set of predefined tasks and task-based policies that let you run DeskView Client Tools from the Symantec Management Console. However, if you want to customize the way a DeskView Client Tool runs, you can run the tool using a customized command line. You can use the script task to run DeskView Client tools using a command line.

The command-line syntax and parameters are listed in the *DeskView Client 6 User Manual*, under the DeskView Client Components chapter. For your convenience, this document is included into the DeskView installation. You can find the *DeskView Client 6 User Manual* in the Symantec Management Console (click **Help > Documentation Library**). You can also download the document from the following Web site: http://ts.fujitsu.com/solutions/it_infrastructure_solutions/manageability/deskview_downloads.html

DeskView includes a sample script task. The task's location is **Home > DeskView > Tasks > DeskView Sample Tasks and Jobs > Set BIOS Settings to predefined (local use) values**.

To run a DeskView Client Tool using a command line

1. In the Symantec Management Console, on the Manage menu, click **Jobs and Tasks**.
2. In the left pane, click **Client Tasks > DeskView**.
3. Right-click the **DeskView** folder.
4. In the right-click menu, click **New > Task**.
5. In the Create New Task dialog box, in the left pane, click **Run Script**.
6. In the right pane, type a new name for the script.

7. Click **OK**.
   This creates a new script task.
8. On the script task page, in the Script type drop-down list, click **Command Script**.
9. Under Script Details, type the commands you want to execute on the target client system.
   For more information, see the *DeskView Client 6 User Manual.*
10. (Optional) Configure the other settings.
    For help, in the Symantec Management Console, press **F1** or click **Help > Context**
11. Click **Save changes**.
12. Run the task one time or on a schedule.
    For information on running tasks, see the *Symantec Management Platform Help.*

Using DeskView Alarm Management

DeskView Alarm Management let you monitor the hardware and software status of the client systems and receive alerts in the Symantec Management Console when the status changes.

For example, you can configure the client systems to report changes in the S.M.A.R.T. status of their hard drives. S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) is a diagnostic system integrated into the hard disk, which monitors important parameters, such as temperature, running performance, and data throughput at all times. Receiving early S.M.A.R.T. alerts will help you identify failing hard drives before they become unreadable and important data is lost.

You can also configure DeskView to send you an email when a DeskView Notification is received.

For details about available notifications, see Configure General Notification Selection page on page 54.

To configure and start using DeskView Notifications, perform the following steps:

Step	Action	Description
Step 1	Configure the Notification Server computer.	You must configure the DCOM protocol on the computer where you installed the Symantec Management Platform. See Configuring the Notification Server computer on page 33.
Step 2	Select the notification you want to receive.	Various hardware and software notifications are available. See Selecting notifications on page 33.
Step 3	(Optional) Configure notifications email forwarding.	When a notification is received, DeskView will forward it to your email. See Forwarding notifications by email on page 34.

Step	Action	Description
Step 4	Enable notifications.	You can enable sending notifications to Notification Server, displaying and logging them on the client computer. See Enabling DeskView notifications on page 34.
Step 5	(Optional) Change the notifications' settings.	For example, you can change the threshold values for free disk space notifications. See Configuring the notification settings on page 34.
Step 6	View DeskView notifications.	You can view notifications, sent by the client systems in the Symantec Management Console. See Viewing DeskView notifications on page 35.

Configuring the Notification Server computer

DeskView clients use the Distributed Component Object Model (DCOM) wire protocol to transmit asynchronous notifications to Notification Server. Microsoft Windows Server introduced enhanced default security settings for the DCOM protocol, which can block DeskView Alarm Management functionality. To enable the reception of DeskView notification on Microsoft Windows Server, configure the DCOM settings using the Component Services snap-in Microsoft Management Console (MMC).

To configure DCOM

1. On the Notification Server computer, click the Windows **Start** button, and then click **Run**.
2. Type `dcomcnfg` and click OK.
3. In the Component Services dialog box, in the tree pane, click **Component Services > Computers**.
4. In the results pane, right-click **My Computer**, and then click **Properties**.
5. On the COM Security tab, under Launch and Activation Permissions, click **Edit Limits**.
6. In the Launch Permission dialog box, add the group **NETWORK**.
7. Set the following permissions for the NETWORK group to "Allow":
   - Remote Launch
   - Remote Activation
8. Click **OK**.

Selecting notifications

You can select the notifications you want to be informed about.

To select notifications

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Configuration > DeskView Notifications > Notifications Settings > Configure General Notification Selection**.
3. In the right pane, check the notifications you want to be informed about.
   For example, if you want to be notified of the hard drive failures, check the Hard disks (S.M.A.R.T.) notification.
   For help, in the Symantec Management Console, press **F1** or click **Help > Context**
4. Click **Save**.

Forwarding notifications by email

(Optional)

You can configure DeskView to send an email whenever a notification occurs.

To configure notifications forwarding

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Configuration > DeskView Notifications > Notification Forwarding > Configure General Notification Email Forwarding**.
3. In the right pane, check **Active**, and fill in the fields.
   For help, in the Symantec Management Console, press **F1** or click **Help > Context**
4. Click **Save**.

Enabling DeskView notifications

You can enable DeskView notifications using the Enable/Disable Notifications policy.

To enable DeskView notifications

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Configuration > DeskView Alarm Management > Notifications Settings > DeskView Enable/Disable Notifications policy**.
3. In the right pane, check **Notifications enabled**.
4. (Optional) Configure other settings.
   For help, in the Symantec Management Console, press **F1** or click **Help > Context**
5. Turn on the policy.
   To turn on the policy, at the upper right of the page, click the colored circle, and then click **On**.
6. Click **Save changes**.

Configuring the notification settings

(Optional)

After you enable notifications, you can change the settings for the following notifications:

- For the "Disk free space" and "System disk space" notifications you can change the error and warning threshold values.
- For the "Lease expiration" notification, you can change the lease expiration date and when to display the lease expiration warning.

To configure notification settings using a task-based policy

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Configuration > DeskView Alarm Management > Notifications Settings**.
3. Click the notification you want to configure.
4. In the right pane, configure the settings.
   For help, in the Symantec Management Console, press **F1** or click **Help > Context**
5. Configure the scheduling options.
6. Turn on the policy.
   To turn on the policy, at the upper right of the page, click the colored circle, and then click **On**.
7. Click **Save changes**.

Viewing DeskView notifications

You can view notifications that the client systems sent to Notification Server from the reports or from the Resource Manager.

To view a summary of DeskView notifications

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Reports > Dashboards > DeskView Notifications**.

To view new incoming DeskView notifications

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. In the left pane, click **Reports > Dashboards > DeskView New Notifications**.

To view DeskView notifications for a single computer

1. Open the Resource Manager for a computer.
   See Accessing the Resource Manager on page 37.
2. In the Resource Manager, on the View menu, click **DeskView Notifications**.

Viewing the system data of a DeskView managed system

When a computer has the DeskView Agent installed and sends inventory data to the database, it becomes a DeskView managed system.

You can view the system data of a specific DeskView managed system in the Resource Manager.

See Accessing the Resource Manager on page 37.

You can view the following information on DeskView managed systems:

- Inventory
  See Viewing DeskView inventory on page 37.
- Events
  See Viewing DeskView events on page 37.
- Notifications
  See Viewing DeskView notifications on page 35.
- System data
  See Viewing DeskView System Data on page 38.

Accessing the Resource Manager

In the Resource Manager, DeskView displays information about the target computer.

To open the Resource Manager from computer filters or reports

1. In the Symantec Management Console, on the Home menu, click **DeskView**.
2. Click **Filters**.
3. Click a filter.
   For example, click **Computer Categories> Professional PCs filter**.
4. In the right pane, double-click the computer for which you want to open the Resource Manager.
   The Resource Manager opens in a new window.

To open the Resource Manager directly

1. In the Symantec Management Console, on the Actions menu, click **Remote Management > Real-Time Management**.
2. On the Manage page, enter the host name or the IP of the computer for which you want to open the Resource Manager, and then click **Connect**.

Viewing DeskView inventory

You can view the inventory collected by the DeskView agents in the Resource Manager.

To view DeskView inventory

1. Open the Resource Manager window for the computer.
   See Accessing the Resource Manager on page 37.
2. On the View menu, click **Inventory**.
3. In the tree view pane, expand one of the following folders:
   - DeskView System Data
     This folder shows system data that is reported by the DeskView Agent.
   - DeskView System Settings
     This folder shows system settings that are reported by the DeskView Agent.
4. Click the item you want to view.

Viewing DeskView events

You can use the Resource Manager to track DeskView events, such as Client Tools events, DeskView setup events, and DeskView Agent events.

To view DeskView events

1. Open the Resource Manager window for the computer.
   See Accessing the Resource Manager on page 37.
2. On the View menu, click **Events**.
3. In the tree view pane, expand the DeskView Events folder.
4. Click the item you want to view.

Viewing DeskView System Data

The DeskView System Data page displays the following system data:

- Summary
- Details
- Mainboard
- Graphics
- Network
- Drives
- Software
- Characteristics

To view DeskView System Data

1. Open the Resource Manager window for the computer.
   See Accessing the Resource Manager on page 37.
2. On the View menu, click **DeskView System Data**.
   For help, on the DeskView System Data page press **F1** or click **Help > Context**.

Chapter 7
Further help topics

This chapter includes the following topics:

- *DeskView BIOS Management tool*
- *DeskView Energy Management tool: Change Power State task*
- *DeskView Energy Management tool: Change power scheme settings task*
- *DeskView Driver Management tool: Update drivers task*
- *DeskView Security tool: Configure Mass Storage Access task*
- *DeskView Alarm Management*
- *DeskView Serial Numbers tool*
- *DeskView System Data page*
- *DeskView Notifications page*
- *Cleanup Inventory Cache task*

DeskView BIOS Management tool

This section includes the following topics:

- *Archive BIOS task*
- *Update BIOS task*
- *Update BIOS settings task*
- *Update processor microcodes task*

Archive BIOS task

This task archives the BIOS together with the BIOS setup settings and microcode patches.

See *Archiving and updating BIOS and BIOS settings* on page 20.

You can use the BIOS archive files that you create with this task to deploy the identical BIOS settings to other systems.

See *Using DeskView BIOS Management to harmonize BIOS settings in your environment* on page 21.

Note
You must run DeskView BIOS Management tools under an administrative user or system account.

The following options are available on this page:

Option	Description
Path	
Directory	Click if you want to store BIOS archive files in a custom working directory. Type the path for the custom working directory. We recommend that you type a network share. Example: `\\server\share` You can also specify a directory on the client system. Example: `C:\BIOS_update_files\`
Store on the Notification Server computer	Click if you want to store BIOS archive files at the default storage that is located on the Notification Server computer. This option lets you store BIOS archive files on the Notification Server computer by using the system account.
File name	
Automatic	Click to create the file with the name based on the internal name syntax (systemname_mainboardname_date_time.bup). Example: `MYPC_D1837_12-12-2008_110000.BUP`
Specify name or pattern	Click to create the file with a custom name. Specify the name of the BIOS archive file. You can create the file with a name according to the pattern specified. You can use the following variables: ● #domain# = System domain ● #name# = Computer name ● #system# = System board (mainboard) ● #date# = Current date ● #time# = Current time in the format HHMMSS ● #no# = Automatically generated serial number You can mix fixed name components and variables. Example: `MyArch_#name#_#date#.bup`
Overwrite existing archive	Check to overwrite the archive if a file with the same name already exists in the directory you specified.

Option	Description
User interaction	
Show warning during archive	Check to show a warning message on the system whose BIOS is being archived.
Execution environment	
Run with rights	Select a user with administrative privileges.

Update BIOS task

This task lets you update the system BIOS.

See *Archiving and updating BIOS and BIOS settings* on page 20.

If you use the BIOS archive file that was previously created using the Archive BIOS task, then the Update BIOS task modifies both the BIOS setup settings and microcode patches.

If you use the BIOS update file provided by Fujitsu Technology Solutions, the BIOS setup settings are not modified.

Note
You must run DeskView BIOS Management tools under an administrative user or system account.

The following options are available on this page:

Option	Description
BIOS update file	
Get BIOS Update Files from	Click if you want the client systems to use the BIOS update file located at a specific location. For example, you can specify a network share. Example: `\\server\share` Make sure this share is accessible by all client computers and available until the last computer has run the task. You can also specify a directory on the client system. Example: `C:\BIOS_update_files\`
Automatically select matching file	Click to detect the BIOS update file automatically. DeskFlash can select the appropriate BIOS update file if there is more than one BIOS update file in a directory. This option can slightly increase network traffic.
Specify filename	Click if you want to specify the BIOS update file manually. Example: D1837*.bup
BIOS Management Job	

Option	Description
Update BIOS code (and archived settings)	Check if you want to update the BIOS on client system.
Allow to overwrite BIOS by older or equal version	Check if you want to overwrite the BIOS on the client system, even if the update file does not contain a newer BIOS.
Update BIOS settings from archive	Check if you want to update the BIOS from an existing archive file.
If BIOS version differs, perform complete BIOS update	Check if you want to completely update the BIOS if the versions are different.
Battery Load	
Minimum Battery Load, if running on battery	Set the minimum state of charge from 33% to 100% for the selected action
User Interaction	
Wait for user OK	Click to prompt the local user to accept the task run request. The user will be warned that he should not bring the system to standby or hibernate states before the next restart.
Show warning during flash	Click to run the task immediately. The user will be warned that the task is in progress.
No user interaction	Click to run the task immediately. No message will appear on the client system. Use this option if you run this tool on computers with no users logged on, for example, if you schedule this tool to run at night.
Execution environment	
Run with rights	Select a user with administrative privileges.

Update BIOS settings task

This settings page allows you to set the appropriate BIOS settings within the client machines. In order to set any BIOS setting, select all checkboxes in front of the settings you want to have changed by the task and select the desired values.

If a system BIOS is protected by a password (supervisor password) you have to enter the password in order to change settings.

If you wish that exactly all selected BIOS settings are set successfully you might want to set the checkbox near "Fail the BIOS Settings update if ALL selected can not be set successfully". In this case the complete command will be reported as failed if at least one settings cannot be set. If you do not select this checkbox the command will be reported as successful if at least one of the selected settings can be set successful. Please keep in mind that some of the settings are not available on every client computer model.

Some settings may influence (e.g. Disable USB Host Controller, Enable Front USB) or exclude each other (e.g. Low Power Soft Off and 0-Watt PC)

If you have multiple models, it makes sense to create a clone of the task/policy for each computer model you have in your network and adapt the selected settings to this model's possible values.

Be sure to run the command with administrative or system account rights.

The following sections describe the settings available.

Initialize with Default values

This task lets you revert all the values in the BIOS of the client computers to their default settings before all other selected settings are modified. These default values are model specific.

Update BIOS boot order

This task lets you update the BIOS boot order of the client computers. You can specify the sequence of drives or system components that the BIOS will search for during the boot process.

The following options are available on this page:

Option	Description
Boot Sequence	Use the **Add, Remove, Move up,** and **Move down** buttons to specify the sequence of drives and system components that the BIOS searches for during the boot process to start the operating system. Add only the really required devices into the bootorder, because devices which are not present in the client's boot devices list will fail the task.

Update BIOS supervisor password

This task lets you update the BIOS supervisor password of the client computers. The supervisor password prevents unauthorized call up of BIOS Setup. Only those who know the supervisor password can call up BIOS Setup or change BIOS settings remotely.

The following options are available on this page:

Option	Description
New password	Enter a new password. All alphanumerical characters can be used. No differentiation is made between upper-case and lower-case. **Warning** Don’t use the numerical keypad to enter digits.
Confirm password	Re-enter the new password.

Update BIOS user password options (*)

Is accepted by the system for the Password on Boot option as an alternative to setup password. Some systems enable Password on Boot automatically as soon as a user password has been assigned. See also "Update Password on boot options".

The following options are available on this page:

Option	Description
New password	Enter a new password. All alphanumerical characters can be used. No differentiation is made between upper-case and lower-case. **Length:** The maximum password length is system-dependent and can be queried via the WMI instance BiosUserPasswordLength of the class CABG_BIOS_SETTINGS in namespace root\abg1v2\dv_bios. **Values:** Letters A-Z Digits 0-9 **Warning** Don’t use the numerical keypad to enter digits.
Confirm password	Re-enter the new password.

Update HardDisk password options (*)

Prevents the hard disk from being used in another system unless the password is known. The BIOS can also request the password from the user on starting the system. See also "Update Harddisk Password on boot options".

The following options are available on this page:

Option	Description
Existing Password	Enter the existing Harddisk password.
New password	Enter a new password. All alphanumerical characters can be used. No differentiation is made between upper-case and lower-case. **Length:** The maximum password length is system-dependent and can be queried on supported systems via the WMI instance HarddiskPasswordLength of the class CABG_BIOS_SETTINGS n namespace root\abg1v2\dv_bios. **Values:** Letters A-Z Digits 0-9 If more than one harddisk exist, all harddisks get the same password! **Warning** Don’t use the numerical keypad to enter digits.
Confirm password	Re-enter the new password.

Update HDD password on boot options

Enables or disables Password on Boot function. To be able to read the hard disks, it is necessary to enter the HDD password or passwords. If the function is disabled, the BIOS provides the hard disk with the password, provided it has been set on this system.

Option	Description
Update HDD password on boot options	**Values:** Enable or Disable

Update Password on boot options

Enables or disables Password on Boot function. To start the system, the setup or user password must be entered. On some systems this function is enabled when a user password is assigned.

Option	Description
Update Password on boot options	**Values:** Enable or Disable

Update Trusted Platform Module (TPM) state (*)

Sets the status of the TPM module. In the "Disabled" status, the module rejects TPM requests. It can also be managed by the operating system and, for example, be enabled by entering the TPM user password.

Option	Description
Update Trusted Platform Module (TPM) state(*)	**Values:** Enable or Disable

Update Trusted Platform Module hardware (*)

Enables or disables the "Trusted Platform Module" hardware. In the "Disabled" status the operating system does not recognize the module.

The following options are available on this page:

Option	Description
TPM Hardware	Choose the configuration of the TPM hardware on the client computers. Disable: TPM hardware is invisible. Enable: TPM hardware is visible.

Update 0-Watt PC options

This task lets you enable or disable the 0-Watt PC options or specify a time interval in which the client computers can be remotely managed. Enabling the 0-Watt PC option means that the power consumption in switched-off state is reduced to 0 Watt (Green PC).

The following options are available on this page:

Option	Description
Settings for a switched off 0 Watt PC	Select if you want to enable, disable or configure the 0-Watt PC options on the client computers. Enable 0-Watt Feature: The power consumption is 0-Watt (Green-PC). In this state the computer cannot be remotely woken and administered. Disable 0-Watt Feature: The computer can be remotely woken and administered. Enable Remote Management: On this setting a time must be specified at which point the computer must switch from power-saving mode into administrative mode. Also a time must be specified at which point the computer must switch from administered mode into power-saving mode. Both time formats are hh:mm (hours:minutes) Note that the allowed values for the time fields need to be in the range from 00:00 to 23:59. In addition the entries for both time fields need to be different.

Update processor microcodes task

This task lets you update the processor microcodes.

See *Archiving and updating BIOS and BIOS settings* on page 20.

Note
You must run DeskView BIOS Management tools under an administrative user or system account.

The following options are available on this page:

Option	Description
BIOS update file	
Get BIOS Update Files from	Click if you want the client systems to use the BIOS update file located at a specific location. For example, you can specify a network share. Example: `\\server\share` Make sure this share is accessible by all client computers and available until the last computer has run the task. You can also specify a directory on the client system. Example: `C:\BIOS_update_files\`

Option	Description
Automatically select matching file	Click to detect the BIOS update file automatically. DeskFlash can select the appropriate BIOS update file if there is more than one BIOS update file in a directory. This option can slightly increase network traffic.
Specify filename	Click if you want to specify the BIOS update file manually. Example: D1837*.bup
Battery Load	
Minimum Battery Load, if running on battery	Set the minimum state of charge from 33% to 100% for the selected action
User Interaction	
Wait for user OK	Click to prompt the local user to accept the task run request. The user will be warned that he should not bring the system to standby or hibernate states before the next restart.
Show warning during flash	Click to run the task immediately. The user will be warned that the task is in progress.
No user interaction	Click to run the task immediately. No message will appear on the client system. Use this option if you run this tool on computers with no users logged on, for example, if you schedule this tool to run at night.
Execution environment	
Run with rights	Select a user with administrative privileges.

DeskView Energy Management tool: Change Power State task

This task lets you turn off, switch into hibernate mode, standby mode or restart a computer.

See *Managing the power state of the client computer* on page 25.

The following options are available on this page:

Option	Description
Restart computer	Click to restart computers.
Shutdown computer	Click to turn off computers.
Switch computer into hibernate mode	Click to switch computer into hibernate mode.

Option	Description
Switch computer into standby mode	Click to switch computer into standby mode.
Terminate all applications currently running without query!	Check to log off the user even if applications are opened on the target computer. All unsaved work will be lost. When not selected, a logoff will not be performed until the user closes all applications.

DeskView Energy Management tool: Change power scheme settings task

This task lets you change the power scheme settings on the target computers.

You must install the Altiris Power Scheme Agent before you can run this task.

See Installing the Altiris Power Scheme Agent on page 17.

Note
Computers that are running the Microsoft Windows 2000, 2003, or XP operating system cannot display custom period values in the Control Panel > Power Options Properties dialog.

DeskView Driver Management tool: Update drivers task

For a stable network, it is indispensable that the system drivers of the client computers are always kept up to date.

With DeskView you can easily update the drivers in two ways:

- Using the Fujitsu Technology Solutions Web site where the drivers are always kept actual
- Using the Fujitsu Technology Solutions Driver and Utility DVD or CD, which contain the driver versions you need for your client computers

This task lets you update system drivers on client computers.

See *Updating drivers on the client systems* on page 27.

The following options are available on this page:

Option	Description
Fujitsu Technology Solutions Web site	Click to download drivers from the Fujitsu Technology Solutions Web site. This option requires the client computers to be connected to the Internet.
Custom directory	Click to load the drivers from a local network share. Type a path to the "DeskView Driver Management" folder of the Fujitsu Technology Solutions Driver and Utility DVD or CD, which contains the driver versions you need for your client computers is located. This option does not require an Internet connection.
Drivers	Select this option to update all Fujitsu Drivers.

Option	Description
System Related Applications	Select this option to update all hardware specific Fujitsu applications.
Fujitsu recommended Windows® Software Updates	Select this option to update all Fujitsu recommended Windows Hotfixes.

DeskView Security tool: Configure Mass Storage Access task

This task lets you lock and unlock removable storage devices of the client computers. You can use this task to prevent data abuse and unintentional bringing in of extraneous software, like viruses or games, from removable storage devices.

This task supports USB mass storage devices on Windows XP and removable disks (flash memory or hard drive based removable disks connected, for example, through USB or FireWire) on Windows 7.

See *Disabling mass storage devices* on page 28.

The following options are available on this page:

Option	Description
Lock mass storage devices	Click to lock all removable storage devices. This action does not lock other USB devices, such as USB keyboard, mouse, or printer. If you want to lock other USB devices, use the Update USB host controller options.
Unlock mass storage devices	Click to unlock all removable storage devices. If you have USB host controller disabled in BIOS, this action will not unlock the controller. Use the Update USB host controller options to unlock the USB host controller.
Set mass storage devices to read only	Click to unlock and set all removable storage devices to read-only mode. This prevents data theft, but does not protect the system against virus attacks. The read-only mode is supported only by Microsoft Windows XP SP2 or later.

DeskView Alarm Management

This section includes the following topics:

- *DeskView Enable/Disable Notifications policy*
- *DeskView Configure Data Disk free space policy*
- *DeskView Configure System disk free space policy*
- *DeskView Configure Lease expiration policy*
- *Configure General Notification Email Forwarding page*
- *Configure General Notification Selection page*

DeskView Enable/Disable Notifications policy

This policy lets you enable client computers sending hardware and software failure notifications to Notification Server.

Additional to DeskView Client notifications, you can configure client computers to send Intel® AMT alerts to Notification Server

See *Using DeskView Alarm Management* on page 32.

The following options are available on this page:

Option	Description
Notifications enabled	Check if you want the client computers to send DeskView Client notifications to the Notification Server computer's IP (shown in the parenthesis).
Local PopUp Window	Check if you want a pop-up window to appear on the client computer when a failure occurs.
Local Log File	Check if you want the notifications to be logged locally on the client computer to a file. The log file is located at "`%DeskView%\Notification\Notifications.log`"
Local System Event Log	Check if you want the notifications to be logged into the client System Event Log.

DeskView Configure Data Disk free space policy

This task lets you configure when the client computers should send an alert to Notification Server.

See *Using DeskView Alarm Management* on page 32.

The following options are available on this page:

Option	Description
Error occurs when free space less than	Set a limit for the minimum amount of free space on the data partition before the error notification is sent.
Warning occurs when free space less than	Set a limit for the minimum amount of free space on the data partition before the warning notification is sent.
Set defaults	Click to reset the values to its defaults.

DeskView Configure System disk free space policy

This task lets you configure when the client computers should send an alert to Notification Server.

See *Using DeskView Alarm Management* on page 32.

The following options are available on this page:

Option	Description
Error occurs when free space less than	Set a limit for the minimum amount of free space on the system partition before the error notification is sent.
Warning occurs when free space less than	Set a limit for the minimum amount of free space on the system partition before the warning notification is sent.
Set defaults	Click to reset the values to its defaults.

DeskView Configure Lease expiration policy

This task lets you configure the lease expiration date value on the client computers.

See *Using DeskView Alarm Management* on page 32.

The following options are available on this page:

Option	Description
Expiration date	Set the lease expiration date.
Display expiration warning	Check to display the lease expiration warning message on the client computer and specify the number of days before the lease expiration date when the warning should be displayed.

Configure General Notification Email Forwarding page

On this page you can configure email settings for DeskView notifications. An email will be sent using these settings whenever a notification occurs.

See *Using DeskView Alarm Management* on page 32.

The following options are available on this page:

Option	Description
Active	Check to activate forwarding notification to an email.
SMTP Server	Type the IP address or the FQDN of the SMTP server.
From	Type an email address of the sender of the email notification.
To	Type a destination email address. You can separate several addresses by a comma or a semi-colon.
CC	(Optional) Type an email address where you want to send a carbon copy of the email notification.
Subject	Type what you want to be displayed in the subject line of the email.
Message language	Select which language you want to send the notification in.
Additional text	The following notification details are sent by email: • computer name • IP address • date • time • event • whether an improvement or a deterioration has taken place • the current status If you want, type additional text here and it will be attached to the message.
Save	Click to save the settings.
Reset	Click to reset to the last saved settings and ignore the changes.

Configure General Notification Selection page

On this page you can configure which notifications you want the client systems to send to Notification Server.

See *Using DeskView Alarm Management* on page 32.

The following options are available on this page:

Option	Description
Autostart Monitoring	This will monitor changes on the autostart setup.
BIOS settings change	This will monitor all changes to the BIOS settings properties.
Cover opening	If the computer is equipped with a sensor for cover opening, the system can check whether the cover was opened or is presently open.
Cover sensor	Indicates whether a cover opening can be detected.
Device changes	Checks the device changes on the IDE and SCSI interfaces.
Display Change	Checks whether the display has been removed, replaced by another display, or an additional display has been connected to the computer (Does not apply to notebook computers).
Fan deterioration	Checks whether the actual rotational speed of the CPU and power supply fan is within tolerances.
Fan monitoring	Checks whether the controller and its CPU and power supply fan function correctly.
Free hard disk space (data)	Checks the free memory space for data on all existing hard disks except the system drive.
Hard disks (S.M.A.R.T.)	Checks the hard disk drives with Self Monitoring And Reporting Technology.
Free hard disk space (system)	Checks the free memory space on the system drive.
Internal short circuit	Monitors the keyboard, mouse, and USB interface for short circuits.
Lease Expiration	Checks the term of the leasing agreement.
Memory changes	Indicates whether the main memory of the system has changed.
Processor change	Checks whether the processor has been replaced with another one or a processor has been removed or an additional process has been installed.
Temperature	Monitors the inside and outside temperature of the computer.
Voltage	Checks whether the 5V voltage, 12V voltage, and the CMOS battery voltage are within tolerances.
Windows Service Monitoring	Monitors the installed Windows Services.

DeskView Serial Numbers tool

This section includes the following topics:

- *Apply imported serial numbers task*
- *Assign single serial number task*
- *Generate serial number task*
- *Manage serial numbers page*

Apply imported serial numbers task

This task lets you assign the serial numbers that you imported into DeskView to the client computers.

For more information on importing serial numbers, see *Managing serial numbers* on page 29.

Assign single serial number task

This task lets you assign a single serial number to a specific computer resource.

The serial number must contain only alphanumeric characters.

See *Managing serial numbers* on page 29.

Generate serial number task

This task lets you generate serial numbers using a specified string pattern.

See *Managing serial numbers* on page 29.

The following options are available on this page:

Option	Description
Serial number pattern	Enter the string pattern for the serial number to be generated. For example, you can type `ABC####`, where `ABC` is the invariable part of the number, and `####` is the sequence that increments each time a client computer requests another serial number.
Serial number range	Type initial and final terms of the sequence.
Override currently assigned serial numbers	Check to let the policy to replace the existing serial numbers on the client computers.
Check range availability	(Task-based policy only) Click to see the number of the DeskView managed resources that need serial numbers and the number of serial numbers that are free.

Manage serial numbers page

On this page, you can create a serial numbers database that you can later assign to systems from Fujitsu Technology Solutions.

See *Managing serial numbers* on page 29.

The following options are available on this page:

Option	Description
View serial numbers	Select to view the list of systems from Fujitsu Technology Solutions, registered with Notification Server, with or without a serial number.
Export serial numbers	Select to export the systems information to a .csv file. You can populate this file with serial numbers using a text editor, and then import the file into the database. Use the Import serial numbers command on this page to import the .csv file. See *Managing serial numbers* on page 29.
Import serial numbers	Select to import the .csv file you created with the Export serial numbers command on this page and populated with serial numbers. To see the resource information you imported, select the View serial numbers command on this page. See *Managing serial numbers* on page 29.
Remove all serial numbers	Select to remove all serial numbers from the serial numbers database.
Remove serial numbers for deleted resources	Select to purge the serial numbers that are not used by existing computer resources.

DeskView System Data page

The DeskView System Data page in the Resource Manager displays the following system and user data for the client computer:

Option	Description
Summary	Shows the system and user data most frequently used by the administrator for the systems that are selected in the Systems pane.
Mainboard	The General section shows manufacturer-specific information about the mainboard and BIOS version. The Processor section shows the processor type and the maximum clock frequency of the processor. The Memory section shows information about the built-in memory modules.
Graphics	The Display section shows the name and serial number of the connected monitor. The Adapter section shows information about the graphic controller.
Network	The General section shows the name of the system and the system administration structure (workgroup, domain, or Active Directory). The Adapter section shows information about the network cards that are installed in the system.
Drives	The Physical Drives section shows information about the built-in drives. Physical drives belong to the system hardware, but they can also be such devices as memory sticks and so on. The Logical Drives section shows information about the logical drives.
Software	Shows information about the operating system, the DeskView version that is installed on the client, and other applications of the system. Not every application that is installed on the system is displayed. Only the applications that you can add or remove using the Control Panel in Windows are displayed.
Characteristics	Shows what types of notification the selected system can send, the current BIOS settings of the selected system, boot order, and the current access settings of removable disks (Windows Vista) and USB Mass Storage Devices (Windows XP).

DeskView Notifications page

The DeskView Alarm Management page displays detailed DeskView Notification data for the selected computer.

See *Using DeskView Alarm Management* on page 32.

The following information is shown for each notification:

Option	Description
Received Time	Shows the date and time when the notification was received by the DeskView Control Center.
Severity	Shows the severity of the event that triggered the notification. The following degrees of severity are possible: • Critical or Fatal • Warning, Minor, or Major • OK • Unknown or Other
Category	Shows the category of the event that triggered the notification. For example, “cover open” or “temperature”.
System	Shows the name of the system that sent the notification.
Processing Status	Shows the processing status of the notification. The following processing states are possible: • New The notification is new and has not yet been processed. • Open The notification is still being processed. • Closed The notification has been processed; processing is complete.

The following detailed notification information is available on this page:

Option	Description
Time of occurrence	Displays the date and time that the event occurred on the system.
Description of event	Describes the reason for the notification.

Option	Description
Additional information	Displays additional information about the corresponding notification and, if applicable, gives advice on error recovery.
Trending information	Compares the severity of the event that triggered the notification with that of the previous notification that was triggered by the same type of event. The trending information is relevant only for events that result in two or more notifications.

Cleanup Inventory Cache task

This task lets you purge the inventory cache that is located on the Notification Server computer. In case of a default DeskView installation, the inventory cache is located at `C:\Program Files\Altiris\DeskView\InventoryCache`.

By default, this task is configured to run daily.

See *Configuring the Inventory Cache purging* on page 18.

The following options are available on this page:

Option	Description
HDD Free Space Limit	Check if you want to purge the cache when the free disk space goes below a specific limit. Type the limit for the minimum amount of free space on the hard disk. Default: 2048 MB
HDD Usage Limit	Check if you want to purge the cache when its size exceeds a specific limit. Type the maximum limit for the amount of cached data that is saved. Default: 10 MB

Appendix A
Glossary

This appendix introduces important terms used in this document.

Symantec Management Agent

The software that is installed on the computers that you want to manage. It facilitates interactions between Notification Server and a managed computer. The agent receives requests for information from Notification Server, sends data to Notification Server, and downloads files. The Symantec Management Agent also lets you install and manage solution plug-ins that add functionality to the agent.

CMDB (Configuration Management Database)

The central database that stores all information about the Symantec Management Platform and its managed computers.

DeskView Agent

The DeskView Agent is software that runs on client computers that can be configured and run remotely using Notification Server task policies. The client software includes a set of the DeskView Client Tools, and an inventory and notification agent (DeskView Agent).

DeskView Client Tools

DeskView Client Tools is a set of tools installed with the DeskView Agent on a client computer. The tools include DeskView BIOS Management, DeskView Energy Management, DeskView BIOS Settings, DeskView Security, and a tool to change the serial number.

DeskView Control Center

The DeskView Control Center (DVCC) consists of a database and central services. All information of the managed systems are stored in the database. All information from DVCC is also transferred to the Altiris Notification Database.

DeskView New Notifications

A page that shows all new incoming notifications. It is refreshed regularly (the default is once a minute). When you start the DeskView New Notification, all notifications not yet processed are displayed.

DeskView Notifications

Alerts that inform administrators about critical conditions, occurred on the client computers.

discovery

The process of searching for computers or other resources on your network that meet specific requirements.

filter

A query that identifies a dynamic group of resources that share common criteria.

Intel AMT (Intel Active Management Technology)

A solution that is implemented in hardware and firmware and is connected to the system's auxiliary power plane. Despite the power state or the operating system state of the client computer, Intel AMT provides IT administrators with access to alerts, hardware inventory, power management, circuit breaker, and agent presence functionality. Intel AMT functionality requires the computer to be plugged into the power source and connected to the network. Intel AMT functionality does not require a software agent to be installed on the client computer.

job

A group of one or more tasks that are run in a particular sequence. Jobs can include conditions that specify when the task runs.

Manageable Systems

The computers that have been discovered by the Discovery Agent and have been identified as systems from Fujitsu Technology Solutions.

Managed Systems

Managed systems are systems from Fujitsu Technology Solutions that have the DeskView Agent installed on them and inventory data has been sent to Notification Server.

Notification Server

The Symantec Management Platform service that communicates with the Symantec Management Agent and the CMDB to provide management, security, and administrative functionality. It processes events, facilitates communications with managed computers, and coordinates the work of the other Symantec Management Platform services.

policy

A set of rules that control the execution of automated actions. Policies can be scheduled or based on incoming data that triggers an immediate action. Policies determine when an action should start and who or what should be notified of the results.

resource

Any item that Notification Server can track or manage, such as a user, site, installed application, computer, switch, router or handheld device.

Resource Manager

A feature that displays information about a resource, such as its properties and current state. It also lets you troubleshoot and perform actions on managed resources.

Symantec Management Console

The Web-based user interface for managing the Symantec Management Platform and any other installed solutions.

task

An action that is performed on a computer. Server tasks are run on Notification Server. Client tasks are run on managed computers.

TPM

Trusted Platform Module.

Index

A

Agent
- Altiris Power Scheme 17
- DeskView 16

Symantec Management Agent
- about 14
- configuring 15
- discovering resources 14
- installing 14

Altiris Power Scheme Agent
- installing 17

B

BIOS
- archiving 20
- configuring settings 22
- disabling interfaces 22
- updating 20
- updating settings 20

C

command line
- using to run client tools 31

computer
- viewing DeskView system data 35

D

DeskFlash tool 20

DeskOff tool 25

DeskUpdate tool 27

DeskView
- about 6
- components 6
- installing agents 15
- Quick Start 12
- system requirements 10

DeskView Agent 7, 20
- installing 16
- viewing installation events 37

DeskView BIOS Settings tool 22

DeskView Energy tool 27

DeskView events
- viewing 37, 37

DeskView inventory
- viewing 37

DeskView Notifications
- configuring 34
- enabling 34
- forwarding by email 34
- selecting 33
- using 32
- viewing 35

DeskView Security tool 28

DeskView Serial Numbers tool 29

DeskView system data
- viewing 38

discovering
- resources 14

documentation resources 8

drivers
- updating 27

E

events
- viewing 37

I

installing
- DeskView 11

inventory
- viewing 37

M

mass storage devices
- disabling and enabling 28

N

notifications
- see DeskView Notifications

P

power management 25

power scheme settings
- configuring 27

purging inventory cache 18

R

Resource Manager 35, 37, 37
- viewing 37

S

serial numbers
- managing 29

SIM 11, 11

Symantec Installation Manager
- see SIM

Symantec Management Console 7, 12

Symantec Management Platform 7, 10

T

tools
- DeskFlash 20
- DeskOff 25
- DeskUpdate 27
- DeskView BIOS Settings 22
- DeskView Energy 27
- DeskView Notifications 32
- DeskView Security 28
- DeskView Serial Numbers 29
- viewing events 37

U

uninstalling
- DeskView 11
- DeskView agents 11
- DeskView software 11

V

viewing events 37

viewing inventory 37